REMARKS/ARGUMENTS

These remarks are submitted in response to the final Office Action of August 10, 2007 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. However, the Examiner is expressly authorized to charge any deficiencies or credit any overpayments to Deposit Account 50-0951.

On the basis of new grounds of rejection noted at page 2 of the Office Action, each of the claims was rejected. Claims 1-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Published Patent Application 2003/0217137 to Roese (hereinafter Roese) in view of U.S. Published Patent Application 2003/0115481 to Baird (hereinafter Baird). Additionally, Claim 19 was rejected under 35 U.S.C. § 112, second paragraph.

Although Applicants respectfully disagree with the rejections, Applicants nevertheless have amended each of the independent claims so as to expedite prosecution of the present application by emphasizing certain aspects of the invention. Applicants respectfully note, however, that the amendments are not intended as, and should not be interpreted as, the surrender of any subject matter. Accordingly, Applicants respectfully reserve the right to present the original version of any of the amended claims in any future divisional or continuation applications from the present application.

Applicants also have amended dependent Claims 6 and 18 to correct a minor typographical error. Applicants have cancelled dependent Claim 19. The claim amendments, as discussed herein, are fully supported throughout the Specification. No new matter has been introduced by virtue of any of the claim amendments.

Certain Aspects Of Applicants' Invention

At this juncture, it may be helpful to reiterate certain aspects of Applicants' invention. One embodiment of the invention, typified by Claim 1, is a method for managing a presentation of sensitive content in non-trusted environments.

The method can include interrogating a list of policies associated with a given user and with a physical device. The method also can include determining a location of the physical device, and comparing the location of the physical device with a list of trusted locations.

Additionally, the method can include providing access to a subscription-based service, which maintains an organization list comprising individuals and machine identification information. The organization list can identify and indicate that a particular individual or machine listed is associated with a predetermined organization. (See, e.g., Specification, paragraph [0019], lines 1-4.)

The method further can include determining that an individual or machine identified on the list is within a predetermined proximity of the physical device. Further according to the method, if it is determined that an individual or machine identified on the list is within a predetermined proximity of the physical device, then an alert can be transmitted to a user via the physical device. (See, e.g., Specification, paragraph [0019], lines 4-9.)

The method also can include enforcing a plurality of rules contained in the policy for managing the presentation of sensitive content. More particularly, the rules can be enforced by blocking a visual presentation or audible presentation of at least one object in portions of the presentation if (1) the physical device is not located in a trusted location, or (2) an individual or a machine identified on the organization list is within a predetermined proximity of the physical device.

The Claims Define Over The References

As already noted above, independent Claims 1, 7, and 13 were rejected as being unpatentable over Roese in view of Baird. Roese is directed to a system that "associates network-lined device with physical locations. (See, e.g., Roese, paragraph [0007].) Baird is directed to system and methods for enforcing access restrictions to network-based documents.

The references fail to teach or suggest a subscription-based service for identifying and indicating individuals or machines identified with a predetermined organization

Applicants respectfully submit, however, that neither Roese nor Baird, taken alone or in combination, teaches or suggests every feature recited in independent Claims 1, 7, and 13. For example, neither reference teaches or suggests providing access to a subscription-based service for maintaining a list of individuals and machines identified with one or more predetermined organizations, as recited in Claims 1, 7, and 13.

Neither reference teaches or suggests determining whether an individual or machine identified with a predetermined organization is within a predetermined proximity

Likewise, neither Roese nor Baird teaches or suggests determining that an individual or machine identified on a list indicating an association with a predetermined organization is within a predetermined proximity of the physical device, as further recited in Claims 1, 7, and 13. Roese is explicitly described as a "location-aware system." (See, e.g., Roese, paragraph [0028], lines 1-4.) Roese looks only to the location of a device. Roese does not consider the device in relation to another machine or an individual, let alone one specifically identified on a subscription-service list as being associated with a particular organization. Conversely, Baird looks exclusively to the access rights of a

particular user or source (i.e., "authorization level") before granting access to a particular document. (See, e.g., Baird, paragraph [0033], lines 1-12; see also FIG. 3.) Like Roese, Baird does not even consider either the location of a device or the device's proximity to a listed individual or machine identified as being associated with a predetermined organization. Accordingly, even when combined, Roese and Baird fail to teach or suggest this feature, explicitly recited in Claims 1, 7, and 13.

Neither reference teaches or suggests alerting a user when an individual or machine identified with a predetermined organization is within a predetermined proximity

It follows, therefore, that neither Roese nor Baird teaches or suggests alerting a user by transmitting an alert to a physical device *if* an individual or machine identified with a predetermined organization is within a predetermine proximity of the device. In a portion of Roese quoted at page 9 of the Office Action, the reference provides:

> For example, secure military and intelligence environments can require that certain physical locations be protected from unauthorized use of computing systems available in that secure location. Each computing system includes a location client that the computing system employs during the process of authenticating an individual user. The expanded location database may contain, for example, attributes such as "secure area" or "minimum security level" truth tables. When a user tries to authenticate, the authentication/location server employs the location of the user requesting authorization when validating credentials. The authentication/location server derives this information, for example, using a reference to a connection point ID as described above. If the user has a security clearance of a high enough level to authenticate from that location, the authentication

process proceeds. If the user fails to meet the security level associated that particular location, then the network can halt the authentication process, sound alarms and/or report the location of the unauthorized user.

In more detail, FIG. 4 illustrates an example process 401 that system 100 employs to determine whether any restrictions to access the network, based on location, are applicable. Specifically, in example location identification process 401 represented by FIG. 4, a user seeking access to system 100 can be first authenticated (step 405) or otherwise filtered by system 100. System 100 achieves this portion of the authorization process by requiring the end user at a location client device to supply certain user information including but not limited to, a name and one or more passwords (e.g., necessary user credentials). If the user is permitted access to system 100 on that basis (e.g., user name and password), system 100 permits the user to query (step 410) system 100 for access to certain information, applications, and the like. Alternatively or in addition, system 100 receives (step 415) the device location before allowing the requested access. A trusted user device (e.g., 104), a network infrastructure device (e.g., a network entry device 114) and/or a location server can supply the user device location using the techniques as described herein. (Roese, paragraphs [0104] and [0105].) (Emphasis supplied.)

As the quoted language reveals, however, Roese looks only to a "security level" of the user seeking to access a document for determining whether or not an alert should be sent. Nowhere does Roese even suggest that the determination of whether or not to transmit an alert should be based on whether or not an individual or a machine identified

with a predetermined organization is within a predetermined proximity of a device, as recited in Claims 1, 7, and 13.

Neither reference teaches or suggests restricting access to portions of a document depending on whether an individual or a machine identified with a predetermine organization is within a predetermined proximity to a device

Since neither reference teaches or suggests determining whether an individual or a machine identified with a predetermined organization is within a predetermined proximity of a device, neither Roese nor Baird provide the necessary ingredients for the other features recited in Claims 1, 7, and 13. Specifically, neither Roese nor Baird even suggest restricting access to portions of a document if an individual or a machine identified on the organization list is determined to be within a predetermined proximity of the physical device, as further recited in Claims 1, 7, and 13.

Accordingly, Roese and Baird, even when combined, fail to teach or suggest every feature recited in Claims 1, 7, and 13. Applicants respectfully submit, therefore, that Claims 1, 7, and 13 each define over the prior art. Applicants further respectfully submit that, whereas each of the remaining claims depends from Claim 1, 7, or 13 while reciting additional features, each of the dependent claims likewise defines over the prior art.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the

Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: October 10 , 2007

Gregory A. Nelson, Registration No. 30,577
Richard A. Hinson, Registration No. 47,652
AKERMAN SENTERFITT
Customer No. 40987
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000